Electronic Signature and PKI Standardisation in Europe

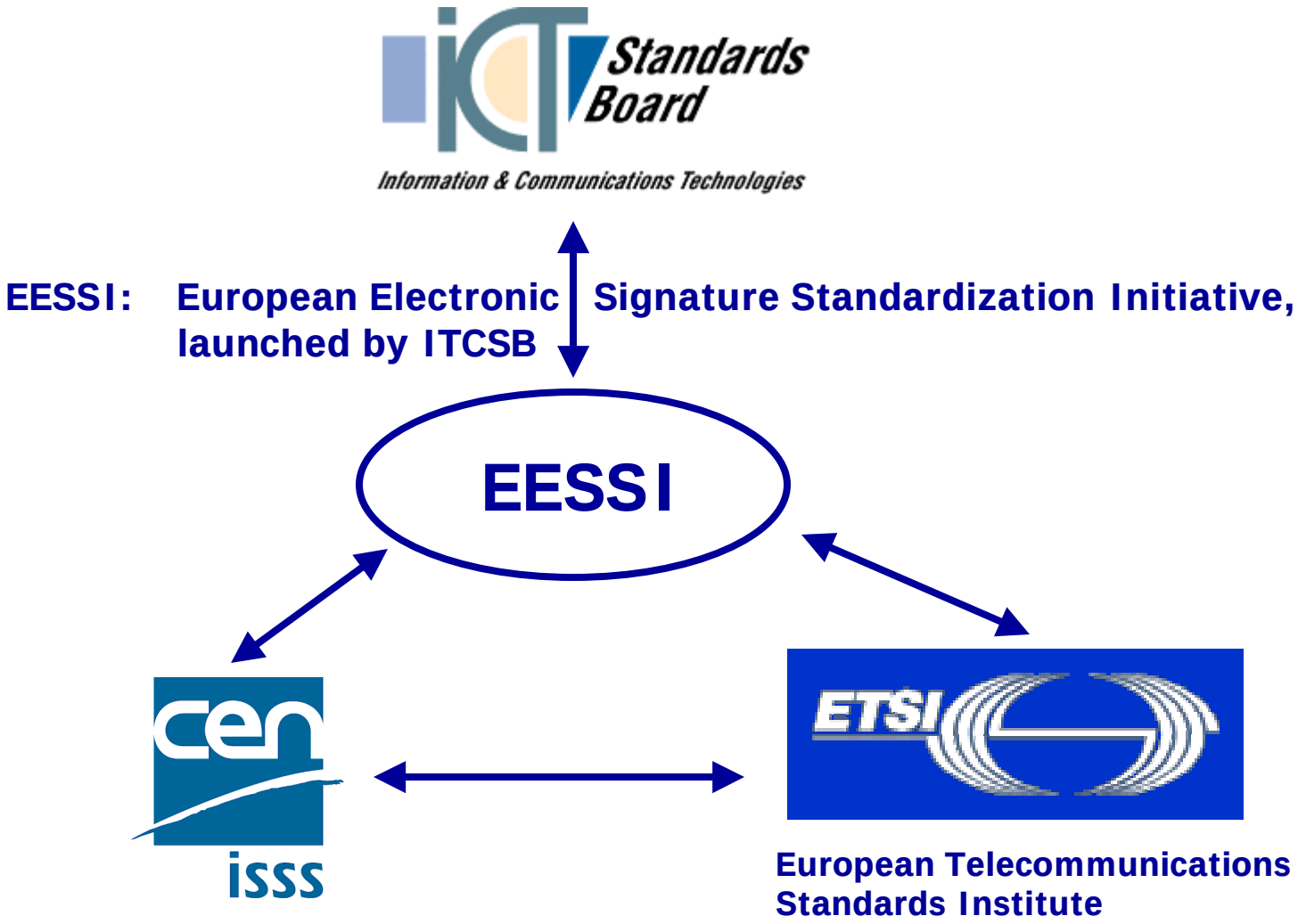
Work-plan & Current Status

FPKI TWG Meeting, 7 June
Gaithersburg

György Endersz, Telia Research AB, Sweden
Chairman ETSI ESI Working Group
gyorgy.g.endersz@telia.se

The Program and the Actors
(Who is Who)

- **EU (European Commission) Electronic Signature Directive** provides a common framework for electronic signatures. Harmonization of the aspects:
  - legal
  - trust
  - technical
- Industry and business, assisted by European standard bodies, will provide a framework for an open, market-oriented implementation of the Directive
- Information & Communications Technologies Standards Board: co-operation between European standards bodies


ICT Standards Board
Information & Communications Technologies
EESSI: European Electronic Signature Standardization Initiative, launched by ITCSB
EESSI
cen
isss
ETSI
European Telecommunications Standards Institute

EESSI Program Implementation

- All deliverables to be published by the end of 2000
- ETSI ESI Working Group
  - 40-50 Participants, funded Specialist Task Force of 8
  - Result: ETSI Standards/Technical Specifications 2-4Q2000
  - Chairman: gyorgy.g.endersz@telia.se
- CEN/ISSS E-SIGN Workshop
  - 70 participants, funded Expert Team of 12
  - Result: CEN Workshop Agreements 3-4Q2000
  - Chairman: hans.nilsson@id2tech.com

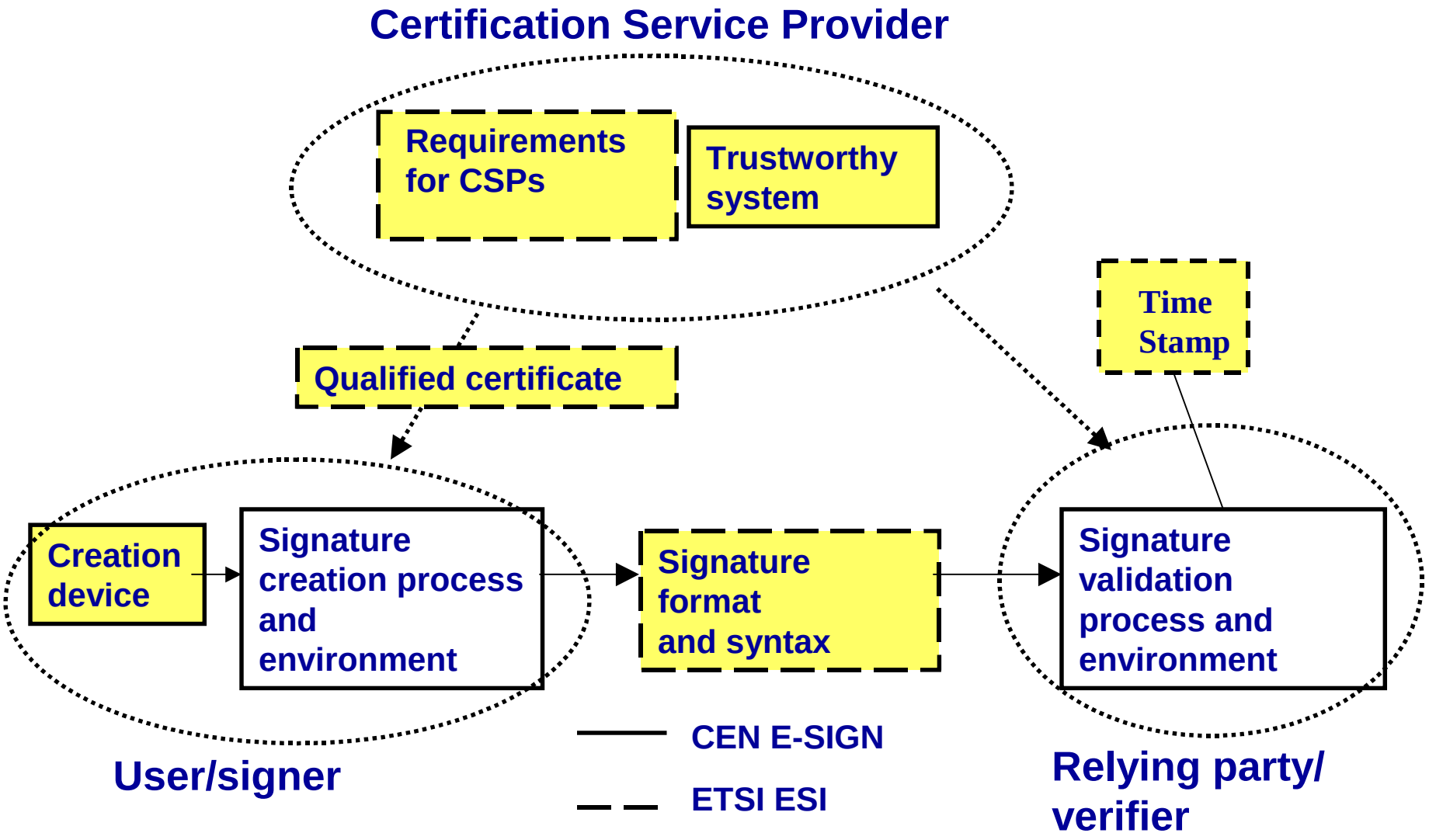
Directive “on a Community framework for electronic signatures, 13 Dec ‘99”

- Ensures legal recognition of electronic signatures
- Security and quality requirements in Annexes I-IV
- Qualified certificates+secure signature-creation device= advanced signatures → hand-written signature
- Other signatures recognised as well (Art 5.2)
- Voluntary accreditation of service providers (tScheme, NL.TTP, Italy, Austria, Germany….)
- Technology-neutral
- To be in place within 18 months

Annexes of the Directive

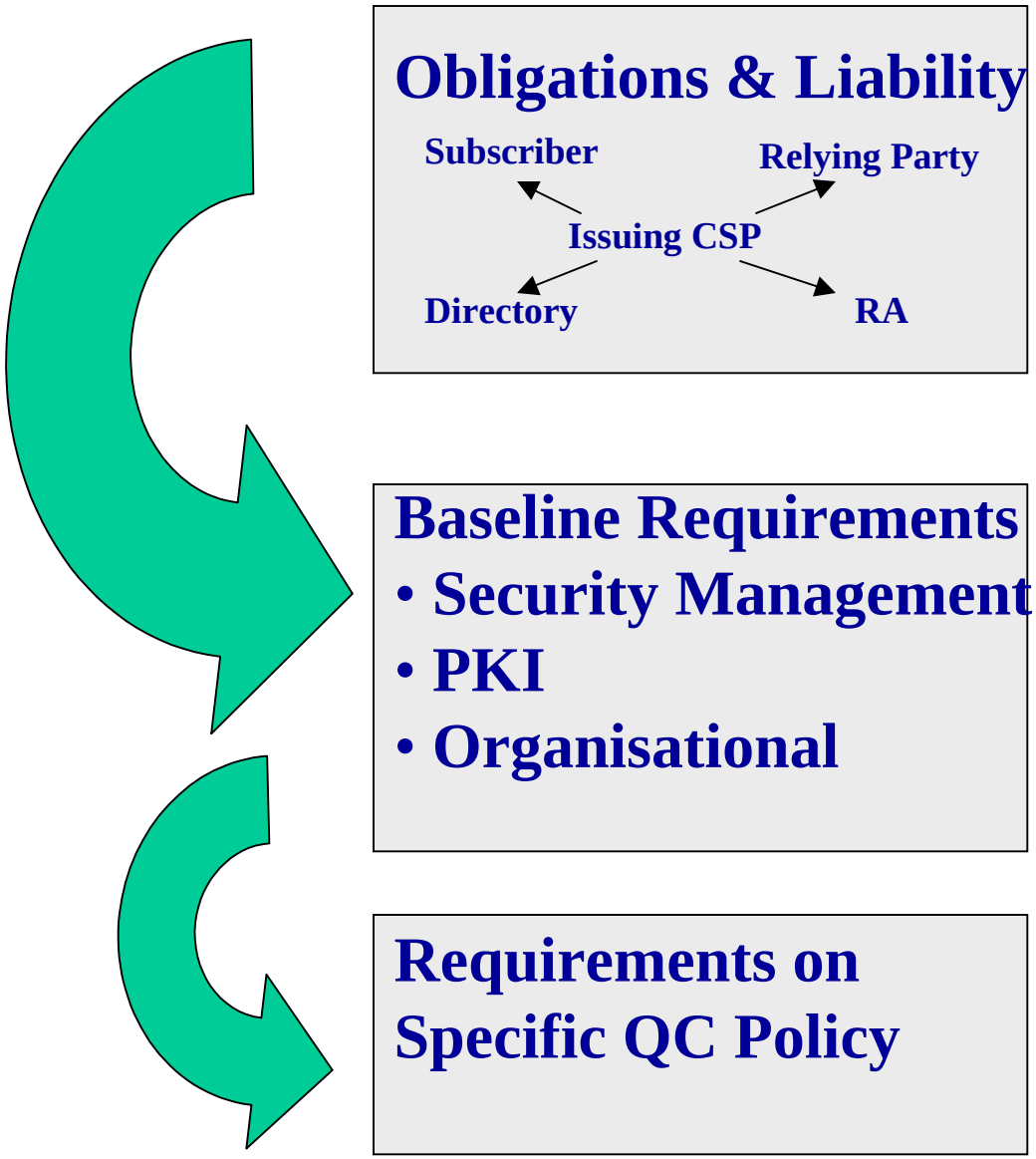
- **Annex I: Requirements for qualified certificates**
- **Annex II: Requirements for certification-service-providers issuing qualified certificates**
- **Annex III: Requirements for secure signature-creation devices**
- **Annex IV: Recommendations for secure signature verification**

EESSI Standards overview



Requirements for Certification Service Providers (CSPs)

- Functional, quality and security requirements expressed in Certificate Policy and security controls
- Consistent requirements to provide the basis for implementation, audit and accreditation
- Current work responds to Directive requirements for CSPs issuing Qualified Certificates, Annex II
- Requirements for other class(es) to meet market needs


Obligations & Liability
Subscriber
Relying Party
Issuing CSP
Directory
RA
Baseline Requirements
• Security Management
• PKI
• Organisational
Requirements on
Specific QC Policy

Requirements for CSPs: Main headings

- **Obligations and liability**
- **Requirements on CSP practice**
  - **CSP Environment**
  - **Key Management Life Cycle**
  - **Certificate Life Cycle**
- **Definition of a specific QC policy**
- **Annex: Cross-references to Directive and to RFC 2527**

Trustworthy Systems for CSPs

Technical security requirements for products and technology components used by CSPs to create certificates for the use of advanced signatures.

To meet security requirements stated in the work area „Requirements for CSPs“. Seek consistent overlap of specifications.

Describe requirements as one or more Protection Profiles using Common Criteria. The use of FIPS 140-1 is considered for the cryptographic module requirements.

Profile for Qualified Certificate (QC)

- Standard for the use of X.509 public key certificates as qualified certificates
- European profile based of current IETF PKIX draft as required by Annex I of the Directive
- Draft to be approved by ETSI SEC in 4Q2000

Qualified Certificate Statements

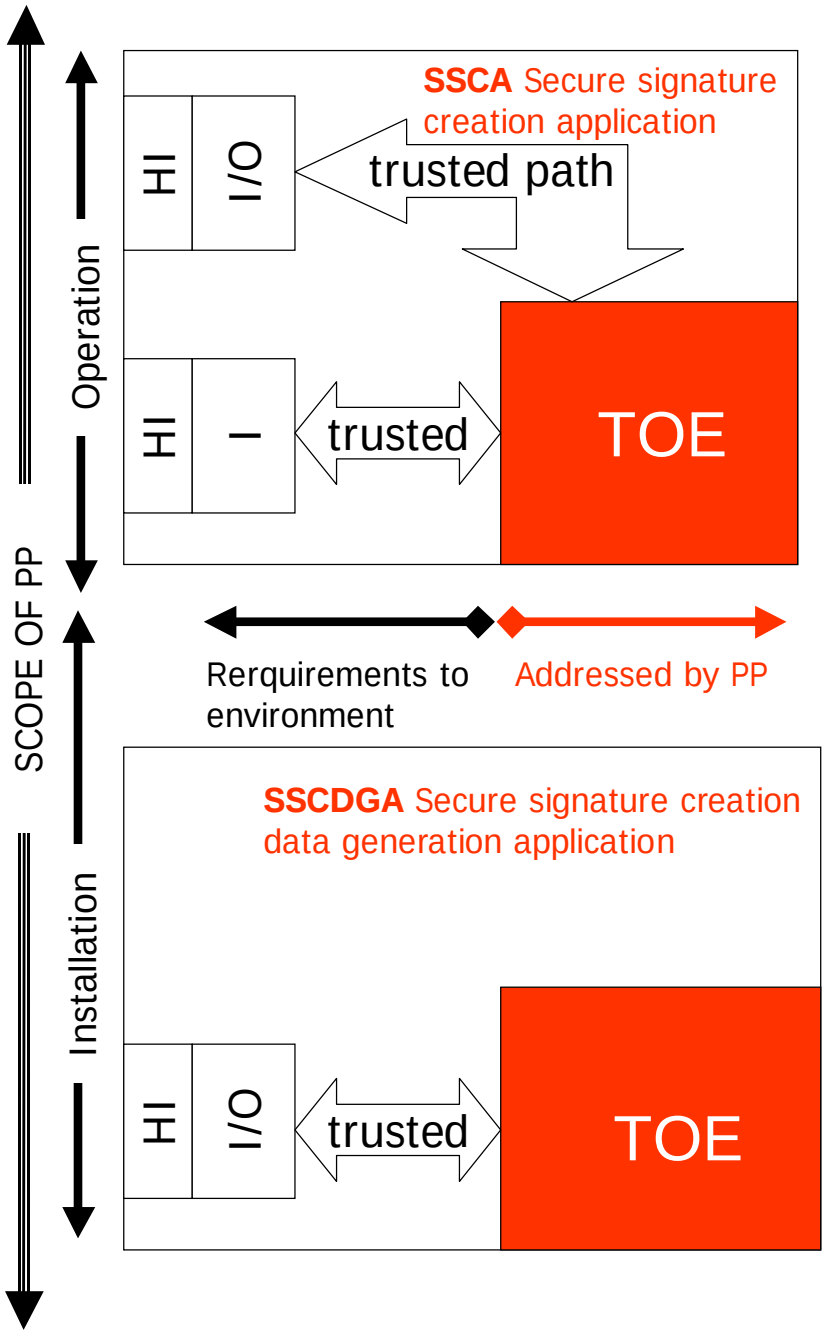
The profile uses the private extension defined in the IETF Qualified Certificates profile, to include the following explicit statements of the Issuer:

- **Statement claiming that the certificates is issued as a Qualified certificate**
- **Statement regarding limits on the value of transactions for which the certificate can be used**
- **Statement regarding the type and identifier of the module protecting the corresponding signature creation device (the private key)**

SSCD: the trusted element at the user

- EU-directive requires SSCD to be evaluated and „confirmed“ by national bodies
- A specific Common Criteria Protection Profile will address appropriateness
- It reflects the requirements regulated in Annex III of the signature Directive
- It is aimed to remain technology neutral as long as security is not impaired
- Use of SSCD to be represented in QC

SSCD: Secure Signature Creation Device



The Scenario

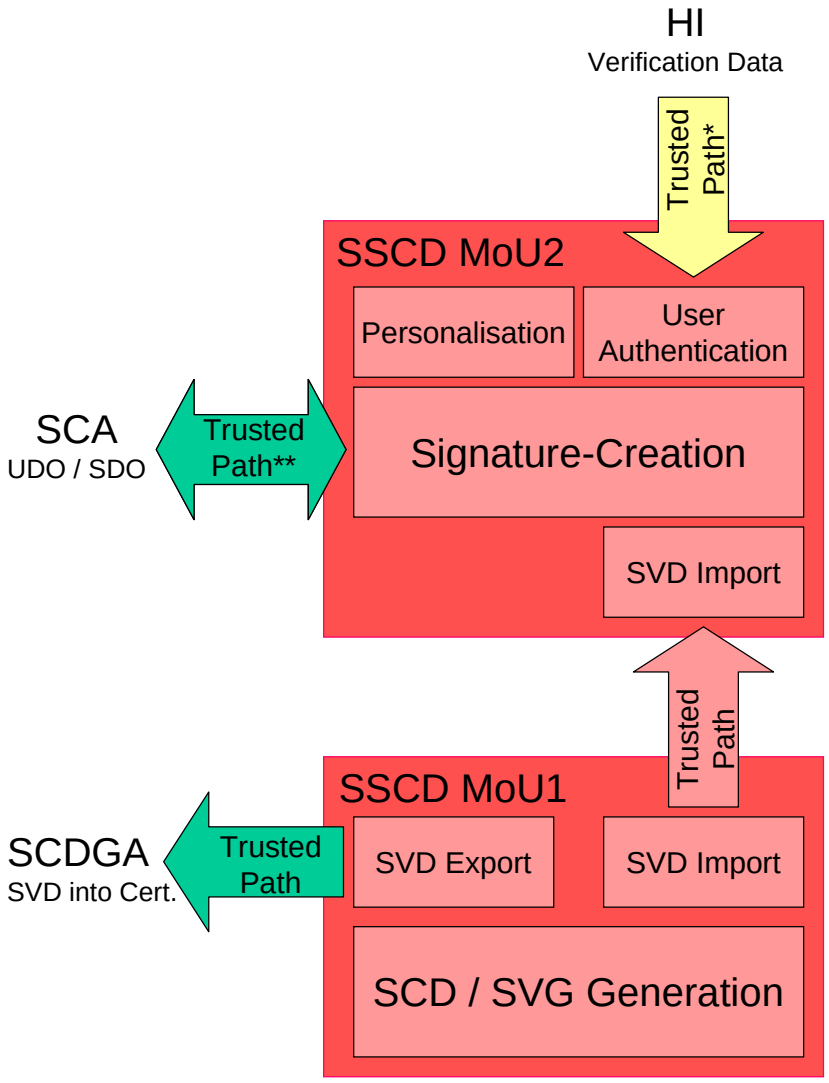
The SSCD is the device „getting in touch“ with the private key.

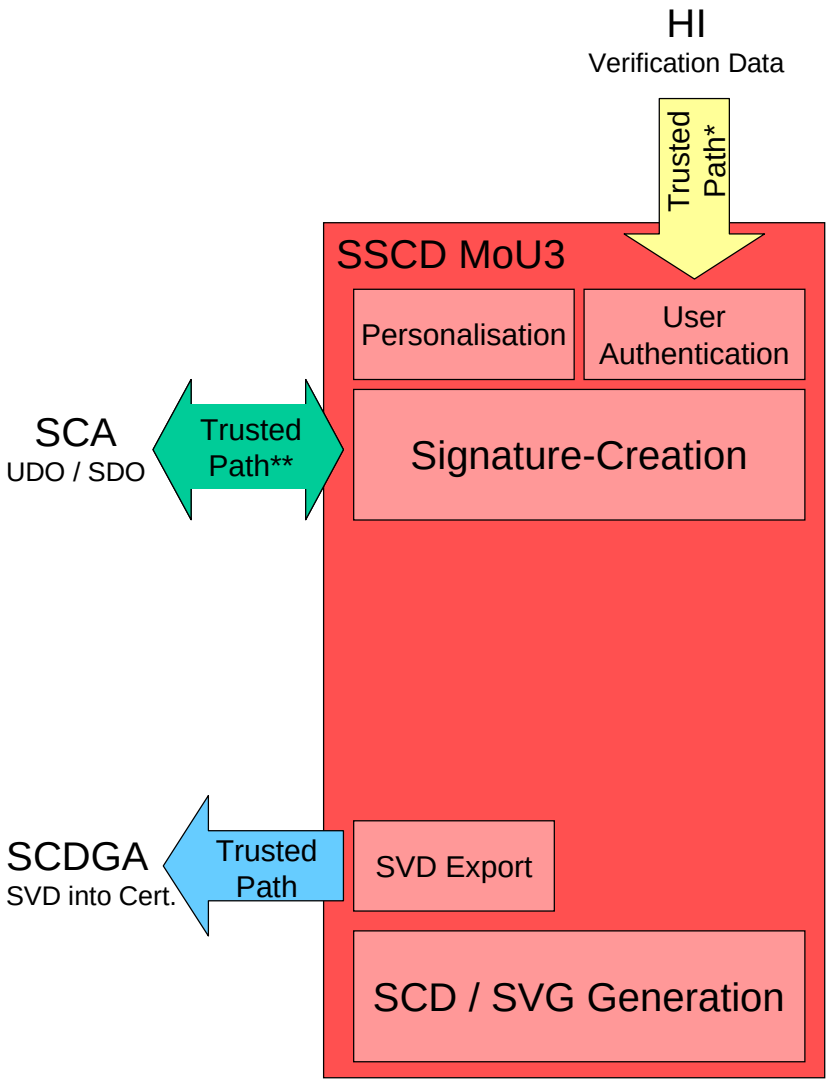
The SSCD comprises the whole lifecycle.

The SSCD assumes an appropriate environment for its application.

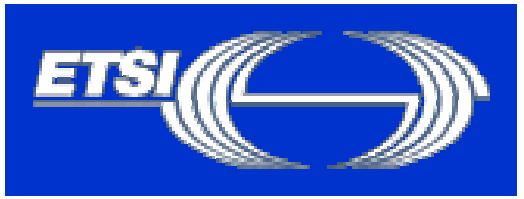
Trusted paths are offered to meet security requirements.

Methods of Use





Electronic Signature (ES) Formats



- Defines interoperable syntax and encoding for signature, validation data and signature policy
  Builds on exiting PKI and digital signature standards
- Published as ETSI Standard (ES) 201 733 in 2Q2000
- Proposed to IETF in March 2000 as an Informational RFC, based on the ES
- Co-operative implementation project in preparation to validate standard and provide software
- Aim: to harmonise development with XML signatures

Forms OF ETSI ES

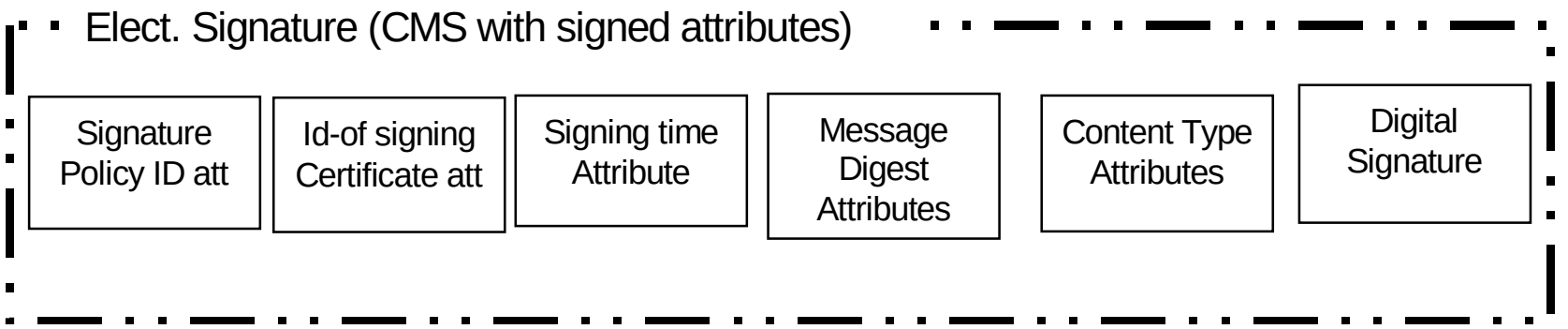
- Electronic Signature (ES), which includes the digital signature and other basic information provided by the signer
- ES with Timestamp (ES-T), which adds a timestamp to the Electronic Signature, to take initial steps towards providing long term validity
- ES with Complete validation data (ES-C), which adds to the ES-T references to the complete set of data supporting the validity of the electronic signature (i.e. revocation status information)
- Extended ES-X to append and/or timestamp PKI verification data
- Archive ES-A to overlay an ES-C or ES-X using stronger algorithms

ETSI ES Signed Attributes

- ETSI ES Mandatory Signed Attributes:
  - Content Type {also mandatory in RFC 2630}
  - Message Digest {also mandatory as RFC 2630}
  - Signing Time
  - Signing Certificate (identification of)
  - Signature Policy Identifier

- This CMS signature structure is generated by the signer
  - Called the ETSI ES (Electronic signature)

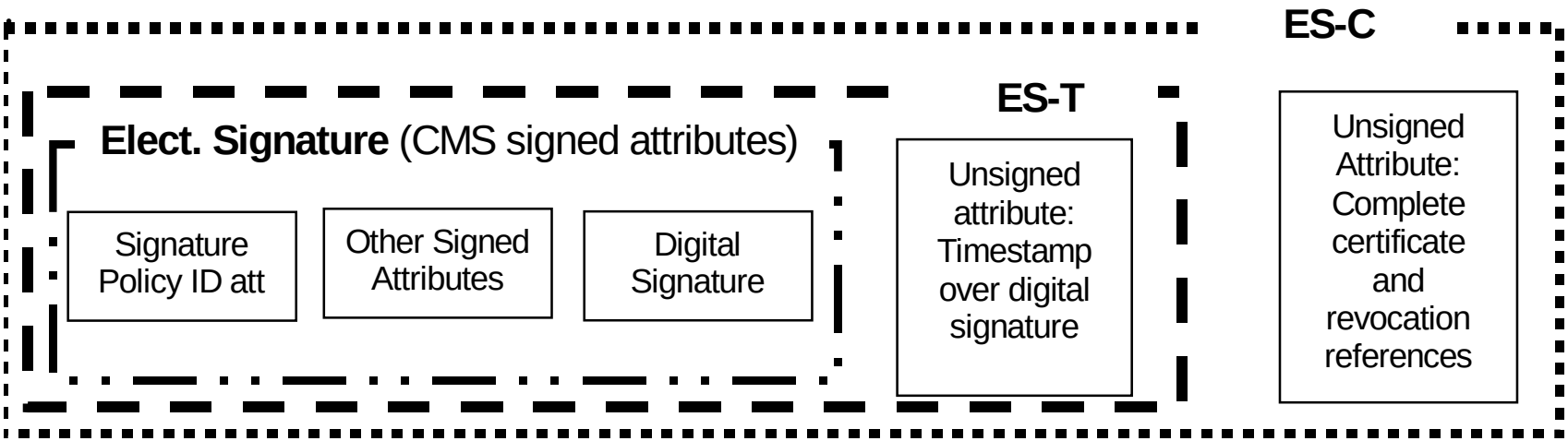
ETSI Electronic Signature
Signers Structures



ES = The ETSI Electronic Signature as generated by the signer.

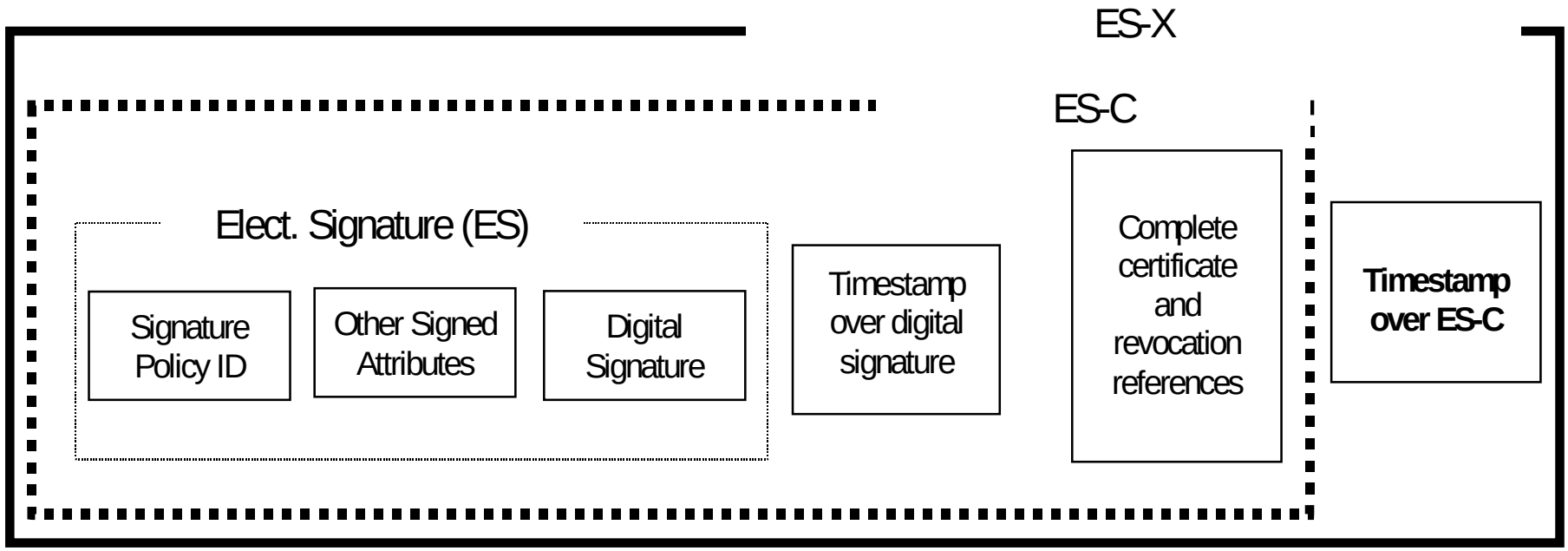
ETSI ES-T and ES-C
Verifiers Structures

Unsigned attributes added for long term verification



ES-T = The ETSI timestamp Electronic Signature
ES-C = The ETSI complete Electronic Signature with references to all information needed to check its validity

Time-stamped ES-C



Format and Protocol for Time Stamp

- Profile based on current IETF PKIX draft
- Time stamps used for signature validation, e.g. in ES 201 733
- Draft to be approved by ETSI SEC in 4Q2000

Issues

- Identification of subjects: in person?
- Naming: the need for unique, permanent, border-less electronic identity
- Management of cryptographic requirements
- How can the relying party verify (on-line) the CA's "living" conformance with the requirements
- Requirements for other than QC: alternative trust levels
- Harmonisation of activities on Signing Policy with IETF and on XML version of ES with W3C
- Timeliness: do IETF drafts for QC and Time Stamp become stable this fall?

Coming Events

- **Stable drafts to be presented at CEN/ISSS and ETSI meetings in Stockholm, 19-21 June. Joint session on Requirements for CSPs, 20 June**
- **Requirements for CSPs available for public comments from ETSI El-Sign Website early July**
- **EESSI full day Workshop in Barcelona, 26 September. Co-located with the Information Security Solutions Europe (ISSE) conference, 27-29 September**

References

- **ETSI:**
  http://www.etsi.org/sec/el-sign.htm
  Sign up from Web-site to open El Sign mailing list

- **CEN:**
  http://www.cenorm.be/isss/workshop/e-sign

- **EESSI:**
  http://www.ict.etsi.org/eessi/EESSI-homepage.htm

- **ISSE Conference & Workshops:**
  http://www.eema.org/isse

Acknowledgements

To my colleagues in the ETSI ESI WG, in particular to John Ross and Nick Pope of Security & Standards (#9, 18-22), and in the CEN E-Sign WS to Reinhard Posch, Universiry of Graz (# 14-16) and Hans Nilsson of iD2, who all have contributed to this presentation in one or another way